DETAILED ACTION

1. Applicant's amendment filed on May 6, 2008 has been entered. Claims 1-35 are pending. Claims 31-35 are cancelled by the applicant.

Supplemental Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given by applicant on August 1, 2008. The applicant has agreed and authorized examiner to incorporate claims 3, 8, 16, 23, and 28 into the independent claims 1, 6, 11, 21, and 26 respectively. In addition, claims 4 and 9 are also amended to be depended on claims 1 and 6 respectively.

CLAIMS:

3. Please cancel claim 3, 8, 16, 23, and 28.

4. Please replace claims 1, 4, 6, 9, 11, 21, 26, and 30 as follows:

Claim 1. A method comprising:

reading an encrypted data block from memory;

regenerating, within a predetermined time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory; and

once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream,

wherein re-generating the keystream comprises: identifying an initial portion of an initialization vector used to encrypt the data block according to a

page containing the encrypted data block; identifying a remaining portion of the initialization vector used to encrypt the data block according to a block number of the data block; and recomputing the keystream according to the identified initial portion of initialization vector and the identified remaining portion of the initialization vector and a secret key.

Claim 4. The method of claim 1, wherein computing the keystream comprises: selecting a stored page initialization vector value according to a page containing the encrypted data block and a block number of the encrypted data block from an on-chip data structure containing one or more unique page initialization vectors; selecting a stored C-bit counter value according to the block number of the encrypted data block; reforming the initialization vector used to encrypt the data block according to the page initialization vector value, the C-bit counter value and (N - C) most significant bits of an address of the encrypted data block, where the address is an N-bit address; and encrypting the formed initialization vector using the secret key to form the keystream.

Claim 6. An article of manufacture including a machine readable storage medium encoded with instructions which may be used to program a system to perform a method, comprising:

reading an encrypted data block from memory;

regenerating, within a predetermined time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory; and

once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream,

wherein prior to receiving the request the method comprises: identifying an initial portion of an initialization vector used to encrypt the data block

according to a page containing the encrypted data block; identifying a remaining portion of the initialization vector used to encrypt the data block according to a block number of the data block; and recomputing the keystream according to the identified initial portion of initialization vector and the identified remaining portion of the initialization vector and a secret key.

Claim 9. The article of manufacture of claim 6, wherein prior to receiving the request the method comprises: selecting a stored page initialization vector value according to a page containing the encrypted data block and a block number of the encrypted data block from an on-chip data structure containing one or more unique page initialization vectors; selecting a stored C-bit counter value according to the block number of the encrypted data block; reforming the initialization vector used to encrypt the data block according to the page initialization vector value, the C-bit counter value and (N - C) most significant bits of an address of the encrypted data block, where the address is an N-bit address; and encrypting the formed initialization vector using the secret key to form the keystream.

Claim 11. A method comprising: computing an initialization vector for a data block according to one or more criteria of the data block, storing the criteria of the data block used to compute the initialization vector for the data block; computing a keystream from the initialization vector and a secret key using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of a memory; encrypting the data block according to the keystream; and storing the encrypted data block within the memory,

wherein combining to form the initialization vector comprises: selecting a stored page initialization vector value according to a page containing the unencrypted data block from an on-chip data structure containing one or more unique page initialization vectors; selecting a stored C-bit counter value according to the block number of the encrypted data block; forming the initialization vector used to encrypt the data block according to the page initialization vector value, the C-bit counter value and (N - C) most significant bits of an address of the encrypted data block, where the

address is an N-bit address; and encrypting the formed initialization vector using the secret key to form the keystream.

Claim 21. A processor comprising: memory encryption logic to store one or more criteria of a data block used to compute an initialization vector for the data block, to encrypt the data block according to a keystream computed from the initialization vector and a secret key, and to store the encrypted data block within memory; and memory decryption logic to regenerate, within a predetermined time required to complete an encrypted data block read, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory and to decrypt the encrypted data block using the regenerated keystream,

wherein the encryption logic further comprises recode logic to identify a data block having a least recent initialization vector, recompute a unique initialization vector for the identified initialization vector, and re-encrypt the identified data block according to a keystream generated from the unique initialization vector and a secret key.

Claim 26. A system comprising: a random access memory (RAM); a chipset coupled to the memory; and a processor coupled to the chipset, the processor including: memory encryption logic to store one or more criteria of a data block used to compute an initialization vector for the data block, to encrypt the data block according to a keystream computed from the initialization vector and a secret key, and store the encrypted data block within the memory, and memory decryption logic to regenerate, within a predetermined time required to complete an encrypted data block read from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory and to decrypt the encrypted data block using the regenerated keystream,

wherein the encryption logic further comprises recode logic to identify a data block having a least recent initialization vector, replace the identified initialization vector with a current initialization vector, and re-encrypt the identified data block according to a keystream generated from the current initialization vector and a secret key.

Claim 30. The system of claim 26, wherein the RAM memory is double data rate (DDR) synchronous data RAM (SDRAM).

Allowable Subject Matter

5. Claims 1,2,4-7,9-15,17-22,24-27,29 and 30 are allowed. The following is an examiner's statement of reasons for allowance: Please see attached interview summary.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2135

TBT
September 29, 2008